Punjab Government Gazette

EXTRAORDINARY

Published by Authority

CHANDIGARH, THURSDAY, AUGUST 6, 2026 (SRAVANA 15, 1948 SAKA)

GOVERNMENT OF PUNJAB

DEPARTMENT OF HOME AFFAIRS

(HOME-4 BRANCH)

NOTIFICATION

The 5th August, 2026

No. Home-HM-40MISC/96/2026-Part(1)/I/1468043/2026.- Whereas the Ministry of Home Affairs, Government of India, vide Letter No. 22003/05/2026-CC dated 09.06.2026, has advised all States and Union Territories to establish and operationalise State Cyber Crime Coordination Centres (S4Cs) as State-level counterparts of the Indian Cyber Crime Coordination Centre (I4C);

And whereas the Department-related Parliamentary Standing Committee on Home Affairs, in its 254th Report, and the Hon'ble Supreme Court of India, vide order dated 01.12.2025 in Suo Motu Writ Petition (Criminal) No. 03 of 2025, have recommended and directed the establishment of S4Cs;

And whereas the Government of Punjab has established the State Cyber Crime Wing, State Cyber Crime Police Station and other specialised cyber-crime units, and considers it expedient to designate the existing State Cyber Crime Wing as the State Cyber Crime Coordination Centre (S4C), Punjab, without creating a new statutory authority or affecting the jurisdiction of existing authorities;

Now, therefore, in exercise of the executive powers conferred by Article 162 of the Constitution of India, the Governor of Punjab is pleased to designate with immediate effect, the existing State Cyber Crime Wing as the State Cyber Crime Coordination Centre (S4C), Punjab, as follows, namely: -

1. Declaration and status.- (i) The existing State Cyber Crime Wing, Punjab, is hereby designated as the State Cyber Crime Coordination Centre (S4C), Punjab.

(ii) The S4C shall function as an administrative, coordination and technical-support mechanism within Punjab Police and shall not constitute a separate Department, Police Station, statutory authority or legal entity.

(iii) This Notification shall not create new posts or establishments, alter sanctioned strength, cadre or service conditions, confer any statutory powers, or entail any additional financial liability.

2. Objective of the State Cyber Crime Coordination Centre.- (i) The S4C shall function as the State-level nodal coordination mechanism for cyber-crime prevention, detection support, investigation support,

prosecution support, cyber-financial-fraud mitigation, cyber-threat analysis, digital forensic support, cyber-security coordination, capacity building, research and public awareness.

(ii) The S4C shall facilitate protection of citizens, Government Departments, public institutions and critical infrastructure by promoting a secure, resilient and trusted cyberspace.

(ii) The S4C shall facilitate effective coordination among Law Enforcement Agencies, the Indian Cyber Crime Coordination Centre, Government Departments, Financial Institutions, the Reserve Bank of India, the National Payments Corporation of India, Telecom Service Providers, Internet Intermediaries, CERT-In (Computer Emergency Response Team in India) and other concerned stakeholders.

(iii) Nothing contained in this Notification shall be construed as conferring upon the S4C any independent statutory power of investigation, search, seizure, arrest, interception, surveillance, blocking of information, attachment of property or prosecution.

(iv) Registration and investigation of criminal cases shall continue to be undertaken by the competent Police Station or investigating agency in accordance with the Bharatiya Nagarik Suraksha Sanhita, 2023, the Information Technology Act, 2000, and other applicable laws.

3. Headquarters and Organisational Structure.- (i) The headquarters of the S4C shall be located at Sahibzada Ajit Singh Nagar (Mohali).

(ii) The S4C shall comprise the following Divisions and Units; namely: -

A. **Cyber Investigation Division:** This division shall provide the functions as core investigational arms of the S4C and shall comprise the following verticals; namely: -

(a) **Cyber Investigation Division (Presently working as State Cyber Crime Police Station):** The State Cyber Crime Police Station shall function as the Cyber Investigation Division of the S4C and shall be the specialised investigation unit for cyber-crime cases within its lawful jurisdiction.

(b) **Proactive Mitigation System (Women & Children)(Presently working as Cyber Crime Prevention against Women and Children (CCPWC)):** The CCPWC Unit shall function as the Proactive Mitigation System for Women and Children and shall be the specialised unit for coordination and technical support in relation to online crimes against women and children.

(c) **State Digital Investigation Support Centre (S-DISC) (Presently working as Digital Investigation Training and Analysis Centre (DITAC):** DITAC shall function as the State Digital Investigation Support Centre (S-DISC) and shall be the specialised digital forensic and technical support unit of the S4C.

B. **Cyber Operations:** This division shall provide the functions as core operational arms of the S4C and shall comprise the following verticals; namely: -

(a) **Emergency Response Division (1930 Call Centre) (Presently working as Citizen Financial Cyber Fraud Reporting System (CFCFRMS)):** The Emergency Response Division shall be the State-level unit for coordination and response to cyber financial fraud incidents. It shall operate on a 24×7 basis from the S4C Headquarters.

(b) **Cyber Threat & Social Media Monitoring Division (Presently working as Social Median Analysis Centre (SMAC) and Cyber Patrolling Unit (CPU)):** The Social Media Analysis Centre and Cyber Patrolling Unit shall function as the Cyber Threat and Social Media Monitoring Division and shall be the specialised unit for cyber threat monitoring and online intelligence analysis.

C. **Cyber Security:** This division shall comprise the following verticals; namely: -

(a) **Cyber Security Division (Presently working as Cyber Security and Intelligence Unit):** The Technical and Support Services (TSS) Wing, Punjab Police is presently functioning as the Nodal Agency for coordination with CERT-In on cyber security-related issues. The Cyber Security Unit, presently functioning under the TSS Wing, shall be transferred to the State Cyber Crime Coordination Centre (S4C) and shall function as the Cyber Security Division to provide cyber security support and cyber threat intelligence. The trained Cyber Commandos posted in the State Cyber Crime Wing, Punjab, shall respond to cyber-attacks within the State.

D. **Administration and Executive Support Division:** This division shall comprise the following verticals; namely: -

(a) **Administration Division (Presently working as Superintendent, Accounts & Administration Branches):** The existing Administrative Branch shall function as the Administration Division and shall be the administrative and establishment support unit of the S4C.

(b) **State Cyber Crime Training Centre (Presently working as DITAC Training Centre, Mohali):** The State Cyber Crime Training Centre shall be the specialised institution for cyber-crime training, professional development and capacity building.

(c) **State Cyber Outreach, Research & Innovation Unit (Presently working as Cyber Awareness Unit):** The Cyber Awareness Unit shall function as the nodal unit of the State Cyber Crime Coordination Centre (S4C) for planning, coordinating and promoting cyber safety and cyber-crime awareness programmes across the State.

(iii) The S4C shall function under the overall supervision and control of the Director General of Police, Punjab.

(iv) The Special Director General of Police/Additional Director General of Police, Cyber Crime, shall be the Head of the S4C and shall be responsible for its administration, coordination and functioning.

(v) The Head of the S4C shall exercise only such administrative and financial powers as may be delegated by the Government or the Director General of Police, Punjab, in accordance with the applicable financial rules, treasury rules, delegation orders, procurement rules and Government instructions, as amended from time to time.

(vi) The Head of the S4C shall be assisted by officers of the rank of Inspector General of Police/ Deputy Inspector General of Police, Superintendent of Police, Deputy Superintendent of Police and such other officers and officials as may be posted or deployed in accordance with the sanctioned establishment.

(vii) The organisational structure shall be as indicated in Annexure "A", and the functional deployment pattern shall be as indicated in Annexure "B".

4. Jurisdiction.- (i) The S4C shall function throughout the State of Punjab as the State-level nodal mechanism for coordination, technical support, cyber-threat analysis, cyber-financial-fraud mitigation, digital forensic assistance, capacity building, research and inter-agency coordination.

(ii) Registration and investigation of criminal cases shall continue to be undertaken by the competent Police Station or investigating agency in accordance with the Bharatiya Nagarik Suraksha Sanhita, 2023, the Information Technology Act, 2000 and other applicable laws.

(iii) The admissibility, proof and evidentiary value of any report or opinion shall be governed by the Bharatiya Sakshya Adhiniyam, 2023 and other applicable laws.

(iv) Requests for blocking public access under Section 69A of the Information Technology Act, 2000, shall be processed only through the competent authority and in accordance with the procedure prescribed under the applicable Rules.

(v) Nothing contained in this Notification shall be construed as—

(a) conferring independent statutory jurisdiction upon the S4C;

(b) altering the territorial or subject-matter jurisdiction of any Police Station, Cyber Crime Police Station or investigating agency;

(c) modifying the legal status, powers or jurisdiction of the State Cyber Crime Police Station, District or Commissionerate Cyber Crime Police Stations, the e-Police Station or Cyber Investigation and Technical Support Units (CI&TSUs);

(d) affecting the powers of any court, statutory authority, regulatory authority or Central or State Government agency; or

(e) superseding any notification establishing a Police Station unless expressly amended by a separate notification issued by the competent authority.

5. Functions of the State Cyber Crime Coordination Centre (S4C).- The S4C shall:-

(a) function as the State-level interface for coordination with the Ministry of Home Affairs and I4C;

(b) facilitate cyber-crime prevention, investigation support and prosecution support;

(c) provide technical, analytical, operational and digital forensic assistance to competent investigating agencies;

(d) facilitate cyber-financial-fraud mitigation and coordination with Banks, Financial Institutions and Payment System Operators;

(e) collect, analyse and disseminate cyber-threat intelligence from lawful sources;

(f) facilitate inter-district, inter-State and inter-agency coordination;

(g) support modernisation and capacity building of Cyber Crime Police Stations and Cyber Investigation and Technical Support Units (CI&TSUs);

(h) facilitate operation of the National Cyber Crime Helpline 1930 and coordination relating to the National Cyber Crime Reporting Portal;

(i) promote training, research, innovation and public awareness;

(j) facilitate cyber-security coordination and incident-response support without prejudice to the functions of Computer Emergency Response Team in India (CERT-In), National Critical Information Infrastructure Protection Centre (NCIIPC), or any other competent authority;

(k) submit such operational, analytical and administrative reports as may be prescribed; and

(l) perform such other lawful coordination and support functions as may be assigned by the Government or the Director General of Police, Punjab.

6. Support to Cyber Investigation and Technical Support Units (CI&TSUs) and Cyber Crime Police Stations.- (a) The S4C shall coordinate and facilitate modernisation and strengthening of the Cyber Investigation and Technical Support Units functioning at the District, Commissionerate and Range levels.

(b) It may facilitate the provision of cyber-investigation tools, digital forensic technologies, technical infrastructure, specialised training, approved Standard Operating Procedures and best-practice material, subject to availability of resources and requisite Government approvals.

(c) Nothing contained herein shall affect the administrative and operational control of the concerned Commissioner of Police, Senior Superintendent of Police, Superintendent of Police or other competent authority over the respective Police Stations and Units.

7. Coordination with the e-Police Station.- The S4C shall coordinate, monitor and provide technical and operational support for the effective functioning of the e-Police Station for registration and processing of e-Zero FIRs relating to cyber-crime offences. The Station House Officer shall register, process and transfer e-Zero FIRs in accordance with applicable laws, Government notifications and approved Standard Operating Procedures (SOPs). The S4C shall facilitate coordination among the e-Police Station, jurisdictional Police Stations, Cyber Crime Police Stations and other concerned units for timely and lawful transfer of e-Zero FIRs.

8. Powers and duties of the Head of S4C:- The Head of the S4C shall,

(i) provide strategic leadership and facilitate coordination among Police Commissionerates, District Police, Cyber Crime Police Stations, specialised units and other law-enforcement agencies;

(ii) oversee lawful collection, analysis and dissemination of cyber-threat intelligence and facilitate lawful preventive, mitigation, investigation-support and response measures;

(iii) act as the State Nodal Officer for coordination with the Ministry of Home Affairs and I4C, subject to Government orders;

(iv) facilitate liaison with Computer Emergency Response Team in India (CERT-In), Reserve Bank of India (RBI), National Payments Corporation of India (NPCI), Banks, Financial Institutions, Telecom Service Providers, Internet Intermediaries and other stakeholders in accordance with applicable law and existing Government-designated nodal arrangements;

(v) facilitate mechanisms for real-time information sharing, digital forensic support, cyber-financial-fraud mitigation, cyber-incident-response support and monitoring of cyber-crime complaints;

(vi) promote research, innovation and studies relating to cyber-crime, cyber security, emerging technologies and international best practices;

(vii) submit recommendations through the Director General of Police, Punjab, to the Government regarding policy, legal, procedural, administrative and technological reforms;

(viii) coordinate with Government Departments, academic and research, industry and other stakeholders for capacity building, research, skill development and cyber-security awareness;

(ix) cause proposals to be processed for engagement of cyber experts, digital forensic specialists, technical consultants, interns and other domain experts, subject to prior approval of the competent authority, availability of sanctioned funds and compliance with recruitment, reservation, procurement, contractual and financial policies;

(x) submit proposals through the Director General of Police, Punjab, for establishment, reorganisation or restructuring of Divisions or Units;

(xi) perform such other lawful functions as may be assigned by the Government or the Director General of Police, Punjab; and

(xii) not restructure or create any organisational unit, creation of a post or additional financial liability shall take effect except with the approval of the competent authority.

9. Manpower and financial implications.- (i) Officers and officials may be assigned, reassigned, deployed or redeployed among the Divisions and Units of the S4C from within the existing sanctioned strength, subject to applicable service rules and orders of the competent authority.

(ii) The staffing pattern indicated in Annexure "B" shall be treated as an indicative functional deployment pattern unless the posts specified therein have been separately sanctioned by the competent authority.

(iii) Annexure "B" shall not, by itself, be construed as .-

(a) sanctioning or creating any post;

(b) enhancing or revising the sanctioned strength;

(c) upgrading or reclassifying any post;

(d) altering any cadre or service condition; or

(e) authorising any additional expenditure.

(iv) Creation of additional posts, enhancement of sanctioned strength or any additional financial commitment shall require separate approval of the competent authority in accordance with applicable service, financial and administrative rules.

(v) Until separate approval is granted, the existing sanctioned establishment shall continue.

10. Reporting and review.- (i) The S4C shall submit periodic operational, analytical, administrative and financial reports to the Director General of Police, Punjab, and the Government, in such form and at such intervals as may be prescribed.

(ii) Its functioning shall be periodically reviewed by the Government.

(iii) Reports required by the Ministry of Home Affairs or I4C shall be furnished through the prescribed channel.

11. Continuity and saving.- (i) The declaration of the State Cyber Crime Wing as S4C shall not affect the legal status, jurisdiction, powers, functions, proceedings, investigations, enquiries, prosecutions, assets, liabilities, contracts, records or administrative actions of—

(a) the State Cyber Crime Wing;

(b) the State Cyber Crime Police Station;

(c) District and Commissionerate Cyber Crime Police Stations;

(d) the e-Police Station;

(e) CI&TSUs; or

(f) any other existing cyber-crime unit.

(ii) Notification No. 11/7/2006-4H(6)/1272 dated 09.06.2009, Notification No. S.O.21/C.A.2/1974/S.2/2024 dated 15.03.2024, Notification No. S.O.33/C.A.46/2023/S.2/2026 dated 15.07.2026, Standing Order No. 1/2011, Standing Order No. 02 of 2024, Standing Order No. 17 of 2024, and other applicable orders and instructions shall continue to remain in force unless expressly amended or superseded by the competent authority.

(iii) References in administrative records to the State Cyber Crime Wing shall, where the context so permits, be construed as references to the State Cyber Crime Coordination Centre, Punjab.

12. Non-derogation.- Nothing contained in this Notification shall derogate from the powers, functions or jurisdiction of Computer Emergency Response Team in India (CERT-In), National Critical Information Infrastructure Protection Centre (NCIIPC), Ministry of Electronics and Information Technology (MeitY), Ministry of Home Affairs (MHA), Reserve Bank of India (RBI), National Payments Corporation of India (NPCI), any court, Police Station, investigating agency or statutory or regulatory authority under any law for the time being in force.

13. Administrative instructions and clarifications.- The Government in the Department of Home Affairs and Justice may issue administrative instructions,implementation frameworks, approved Standard Operating Procedures and clarifications for carrying out the purposes of this Notification:

Provided that no such instruction, framework, procedure or clarification shall—

(1) be inconsistent with any law for the time being in force;

(2) confer any statutory or coercive power not otherwise available under law;

(3) alter the jurisdiction of any Police Station or statutory authority;

(4) create or sanction any post or additional financial liability; or

(5) alter any cadre or service condition without approval of the competent authority.

Sd/-

GURKIRAT KIRPAL SINGH, IAS,

Principal Secretary to Government of Punjab,

Department of Home Affairs.

3792/8-2026/Pb. Govt. Press, S.A.S. Nagar